A Holistic Methodology for Improved RFID Network Lifetime by Advanced Cluster Head Selection using Dragonfly Algorithm

Pramod Singh Rathore[1]*, Abhishek Kumar[2], Vicente García-Díaz[3]

[1] Department of CSE, ACERC Ajmer (India)
[2] Chitkara University Institute of Engineering and Technology, Chitkara University, Punjab (India)
[3] Department of Computer Science, Universidad de Oviedo (Spain)

Received 4 November 2019 | Accepted 9 May 2020 | Published 27 May 2020

Abstract

Radio Frequency Identification (RFID) networks usually require many tags along with readers and computation facilities. Those networks have limitations with respect to computing power and energy consumption. Thus, for saving energy and to make the best use of the resources, networks should operate and be able to recover in an efficient way. This will also reduce the energy expenditure of RFID readers. In this work, the RFID network life span will be enlarged through an energy-efficient cluster-based protocol used together with the Dragonfly algorithm. There are two stages in the processing of the clustering system: the cluster formation from the whole structure and the election of a cluster leader. After completing those procedures, the cluster leader controls the other nodes that are not leaders. The system works with a large energy node that provides an amount of energy while transmitting aggregated data near a base station.

Keywords

Wireless Sensor Networks (WSN), Sensor Nodes (SN), CH Node, Cluster, Cluster Head Selection.

DOI: 10.9781/ijimai.2020.05.003

I. Introduction

RFID is a well-known technology used to identify all kinds of objects. It is a fast-emerging technology that is likely to create massive financial gains in industries and in the digital world. The explanation of the "Internet of Things" concept is usually considered together with the RFID technology. Some of the fields of application include transportation, security, product tracking as well as access control. For the primary purposes, RFID systems can be used to register items, also supporting actions such as counting and tracking objects in motion [1].

The RFID Network protocol is tremendously complex. There is a limitation to design the scheme of any RFID network, being the main constraint the fact of providing power. In addition, diminishing power utilization with the energy consumption process is a significant issue in the intended use of the RFID network protocol. Moreover, RFID systems also have to focus on some aspects such as reliability, scalability or acknowledgment. Therefore, low power RFID readers are used to provide secure and reliable communication. For example, the communication mechanisms can create traffic congestion and they are mostly consuming the resources by transmitting information from the node to the base station. There is a requirement of understanding the process of reducing the burden on the communication mechanism using the straight transmission protocol which is being used for communicating with base station directly [2].

* Corresponding author.
E-mail address: pramodrathore88@gmail.com

In these circumstances, readers are usually separated from the base station and, due to the separation; energy cannot be reflected towards the reader. This separation is the basic reason for high consumption of energy in this particular process. Thus, low power batteries face difficulties in reflecting back the signals to readers. Some authors proposed methods on the MAC and network layers for creating some improvements. However, an important problem is still present when there are more than two nodes that want to act as leaders and confront each other to lead other nodes in the network. Clustering methods are the most important techniques to avoid all difficulties acting in the network [3], [4].

Within the existing system, every reader interprets the data and propel straight near the base station, where it reduces the competence of the readers. In favor of improving good organization of readers in the RFID, the network is based on the cluster method (Fig. 1). In every cluster, we consider the most accurate client and the group of clients which are performing similar operations. Thus, before sending the connection request, the cluster will combine all the related data of the client in advance.

In the proposed work, the RFID network life spans extended by an energy-efficient cluster-based protocol. In addition, with the help of the Dragonfly algorithm, the network life is also extended. This creates a large energy node, like a cluster head, that provides a smaller amount of energy while transmitting aggregated data near the base station. To reduce the loss of energy and to increase the efficiency of the network we need to use the clustering mechanism that can manage complex networks with reduced energy consumption.

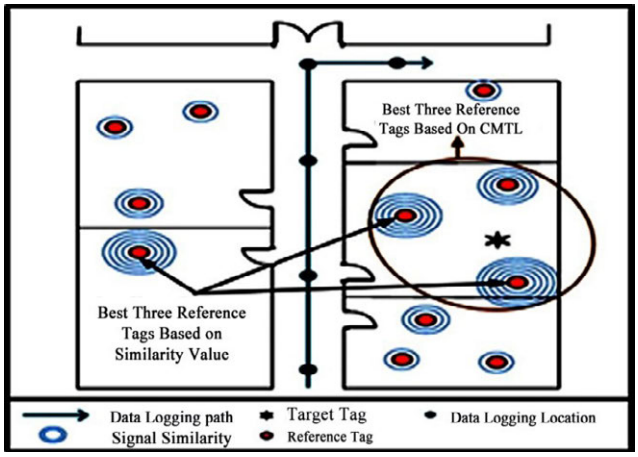

Fig. 1. Cluster-Based RFID Network.

II. Related Work

R. Koh et al. [1] gave a detailed explanation about the establishment of the network and the tracking of the network to identify the packet loss or any kind of miscommunications in between the sender and receiver. The network structure must be maintained nonvolatile and without maintaining any kind of distractions in establishment and the communication. There is a concept mentioned by this author about the Auto -ID which is to track the network including packets which are flowing in the current network. Tracking the system includes the information of the physical device which is a source or destination. In this network, communication source and destination communication devices must be straight forward without any interruption they have to communicate.

J. Kim et al. [2] used the methodologies of the RFID tags to the communication between source and destination which was further used for the reestablishment of the network and also the packet loss. In this scenario we can identify the devices which are connecting in the same network panel. For an example consider the army mission and if the soldiers are connected to the same channel using RFID tags of their device that will be very easy to track the person in any situation. RFID tags are further used for the information processing from source to destination and identifying the receivers based on their tags. Because all the people in the network need not to get the information.

Swimpy Pahuja et al. [5] produced a survey on the RFID tags and the pattern they are communicating among the people and the servers which are connected with the tags will monitor and backup of the communication and the operations are stored as logs. If there is any further same process identified in the same group of network then the same operations and the same log can be referred for the further operations in the network. If we are using the same protocol for the different purpose on the same log the duplication will occur and store the same in the log.

WaleedAlsalih et al. [6] proposed distance-based clustering, which is a technique that is anticipated to reduce the complexity of the network as it takes care of every part of the movements and masking it to make it unaffected from congestion of inactive tags. Shailesh M. et al. [7] suggested a solution for the problem life identifying the collision of the people in the network. If same network was shared between the people, then there will be biggest problem in the network and reconnecting the network or establishing new kind of it. Author suggested new protocols with the new RFID data transmission to recognize the duplication.

The security measures have to be taken very seriously and all the RFID tags must be protected with the latest firewall mechanisms and the information was mentioned in [8]-[10].With low cost we need to mention the security mechanisms and all the mechanisms must be processed according to the willingness of the communicators in the network. Because without any of their intervention nothing must be leaked out of the channel [11], [12].

Routing calculations are being done in this new RFID tags scenario and those are clearly mentioned in [13]. We need to calculate the security levels and proceed further will all kind of operations. Whether it may be secured or unsecured first we need to calculate the channel security and must establish all the related measures. Instead of purchasing the commercial tools it is better to use low cost commodity software or tools for network establishment. That was mentioned on [14]-[16].

Mann et al. presented Bee Swarm, an SI that is based on the energy-efficient hierarchical routing protocol for WSNs [17]. Mirzaie et al. has provided a multi-clustering algorithm that is based on fuzzy logic (MCFL) using a unique methodology that is exhibited to do node clustering in WSN [18].

Elshrkaweyetal., in 2018, proposed an advanced method to minimize energy usage and maximize network lifetime [19]. It needs to support information secrecy, safeguard the WSN and enhance the security. Lalwani et al. [20] presented the biogeography-based energy-saving routing architecture (BERA) for CH selection and routing. Consideration ought to be taken for basic protocols while choosing the CH to improve the life of the system. CSSDA moves further and this movement will require two parts: the first part is the cluster set-up and the second part is the regular cluster. Inside the cluster set up, the reader, who has more enduring power will choose for the cluster heads [21],[22]. The others, which are not chosen for cluster heads, will merge the cluster to their relevant cluster head. Another part is a regular group part, in that each datum established through the cluster heads are combined cumulative and sent toward the base station [23],[24]. In any case, studying the key factors that can be important for the design or routing techniques of wireless networks is a topic of interest in the research community [25].

III. Problem With the Conventional Approach

RFID plays an integral role within the different domains and their requirements are solved with tracking of the person or an object with the RFID tags. If there is a need of tracking animals in the forest, we need to attach a chip to track them. In cases of shopping areas in metro cities, there is no chance of maintaining an inventory of the products and scan them one by one to add in the inventory. In such cases we use these tags to add the bulk of similar products instead of barcodes or QR codes.

The communication channel security at the back end server is one of the most important factors and at the same time tagging the reader messages is necessary for mobile readers. Although, the security issues occur worldwide, and the safety becomes the major issue. This paper means to say that the verification protocol is on the way to ensure that a prohibited tag or reader should break the structure. Hash-based security measure, also unrestricted essential incorruption methods are executed on top of authentication protocol.

We proposed new scalable, anti-counterfeit and undetectable confirmation protocol entrenched in terms of hash method, even public key encryption knowledge for offering the safety and security in RFID tag-reader message procedure. The conventional approach is composed of the following steps:

- De-synchronization. The proposed work eliminates the de-synchronization issue since the server preserves two files of ID (ID also last). Thus, if the message is deemed fraudulent; we know how

to regain it and reverse as of the last ID.

- Anti-counterfeit issue. The Mannequin chip, amid a similar number, is impossible to make when the RFID chip is exclusive. Therefore, a reader might not print identically in order, and our logic is hence explained.
- Forward secrecy. After the modernization of IDi toward IDi+1, there was confusion regarding the one-way encoding method, and there was no other way to produce the original instruction that was ambiguous. That is, IDi+1 cannot create IDi.
- Un-traceability. To track the statement between the entities, using this method, it is hard to compare the two sides, that is the public-key encryption and the time stamp.
- Spoofing. RFID spoofing involves covertly reading and recording a data transmission from a RFID tag. When the data is retransmitted, it would contain the original tag's TID, making it appear to be valid.
- Item privacy. Public, as well as the crucial private encryption decoding, and the encoding of data building is nearly unfeasible to bother the confidentiality of the network.
- Replay attack. Replay attacks build on eavesdropping and specifically occur when one part of communication in an RFID system is recorded and then 'replayed' later to the receiving device in order to steal information or gain access.

IV. Proposed Approach

Through the usage of an energy-efficient cluster-based protocol, the RFID networks may extensively utilize the Dragonfly algorithm during their lifetime (Fig. 2). For every cluster member, the cluster head reader (CH) has a receiver tag charge in order. After, it conveys towards the base station (BS) and executes the aggregation development that received the data. For all RFID Networks, readers obtain the energy stage details from the base station. Under the circumstances, the optimized cluster head is chosen, the base station estimates the average energy levels for every reader presented within the network.

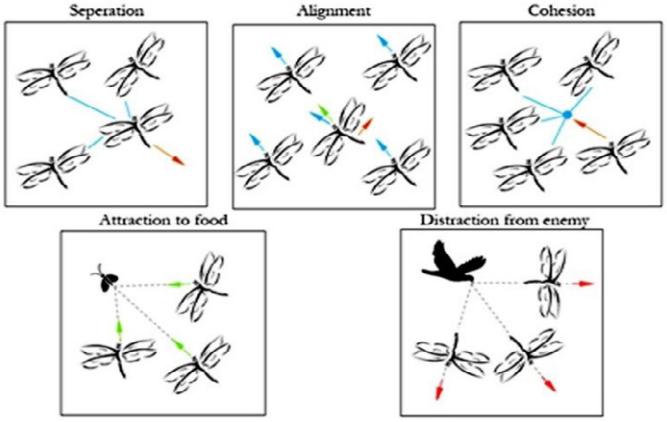

Fig. 2. Structure of the Dragonfly Algorithm.

The cluster head is chosen by the mobile RFID environment where the readers have high power and equivalent mobility, while effect of moving back a few parting readers also increases the network lifetime. On behalf of the dropping movement among the readers into the RFID, the network uses an energy-efficient clustering system. There are two parts of this method. Within the first part, cluster heads are selected on the basis of energy level and mobility of the reader. In the present work the cluster head will be connected to the most ambiguous node which can be solved with connectivity issues of the cluster and the reader can connect to the cluster head easily. Fig. 3 and Fig. 4 illustrate the Cluster Head Selection and the Formation.

The RFID network is enlarging its lifespan through the clustering method. With the aim of energy utilization for every node, the cluster heads are preferred within the clusters. All the readers transmit hello messages in route to their neighbors. In the communication range, every reader reclines and receives the hello message, and recognizes the neighbor and transfer as the reader. Even though inside the network, the entire set of readers may have found their neighbors. With a high probability of attaining, for example, mobility and energy, the cluster heads are chosen. All the readers' energy levels are evaluated among the threshold charge. A threshold value is defined the remaining necessary power get information on or after the entire set of readers aggregates the information and conveys it toward the base station.

Another way to identify a suitable cluster head is by the reader during soaring residual energy that is evaluated to be within the threshold value. Along with the available cluster head, applying Dragonfly Clustering, we choose the optimal cluster heads in the network. After the relevant cluster head is selected, and algorithm of a dragonfly is used. There are three old ethics in the Dragonfly algorithm: i) collision avoidance ii) Segregation iii) nearby Reader's distance.

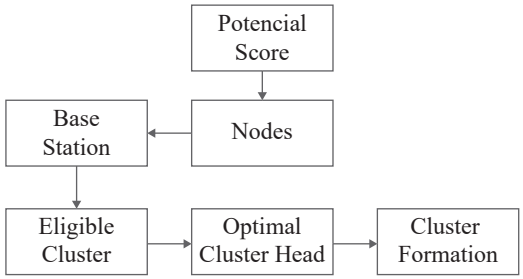

Fig. 3. Dragon Fly Algorithm block diagram.

Distance metrics are used to map the related variables to the specific cluster based on the standard distance metric algorithms. These algorithms identify the similar group elements. Administrators are chosen based on the direction and the speed of the readers that are used for the explanation. The neighbor reader count for every suitable cluster head through a network is known as cohesion. Within the mobile web, there are tags and readers. Given the system, the dynamic behaviors of the readers are three significant features that are worn within the network, the location updates of the nodes are cohesion, alignment and separation. Every element is taken as the best cluster head selection. The paragraph below illustrates that the behaviors are precisely modeled.

Separation: the ambiguity among the cluster head and their neighbor is intended after the cluster head is appropriately elected. To establish a node, it is closely considered by their detachment towards the data transmission in the RFID network. The procedure for separation is given by Eq.(1). The present node location is considered as (x1, y1), whichever reader otherwise tag; the neighboring node location is described as (x2, y2) also neighboring readers, and their count is noted as N between the present reader.

$$S_i = \sqrt{\{(x^2 - x^1)^2 + (y^2 - y^1)^2\}/N} \quad (1)$$

Alignment: after separation, as the moment of the cluster head, the RFID tag can recognize location of the object with respect the specific cluster head. The association of the cluster head should exist in parallel toward neighbor readers in the direction of the cluster headed for evading the RFID network rupture the cluster. Through the alignment, every mobility node is determined. The method of alignment is given by Eq.(2). Everywhere, V_j illustrates what is within the network

mobility of the n-*th* adjacent neighbor node. Later then the speed is choosing the same direction as cluster head direction.

$$A_i = (\sum_{j=1}^{N} V_j)/N \quad (2)$$

Cohesion: when the procedure of alignment is finished, the adjacent neighbor node is intended to favor the appropriate cluster heads. The neighbor nodes is said to be the number of nodes around the cluster head, for which the calculation is not as much of the cluster, which is synchronized, and becomes exaggerated. Therefore, anode must always remain separated to avoid collision; this is useful for the network and their competence. The prescription for cohesion is described in Eq.(3).

$$C_j = (\sum_{j=1}^{N} V_j)/N - X \quad (3)$$

Where, X is the position of the current individual, N is the number of neighborhoods and X_j is the position of the jth neighboring node in the RFID network.

The cohesion, alignment and separation ranges are added for every cluster head. Here, the cluster head will be chosen as a head. Based on low mobility, distance, and neighbor count, the cluster head will be selected.

After the optimal cluster head is chosen (based on the cluster) the cluster head mobility is formed due to the presence of readers and tags. In the network, to avoid the collision and termination of communication amongst the nodes, the cluster head must be selected with majority.

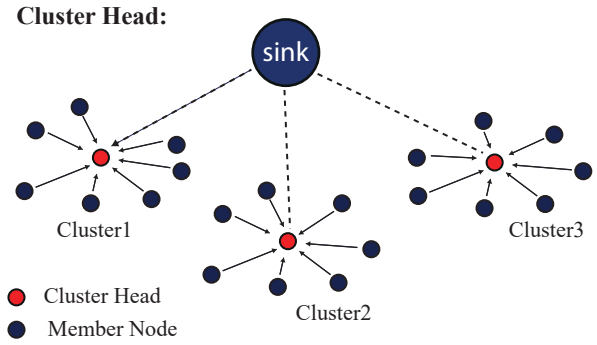

Fig. 4. Dragon fly algorithm representation.

In addition, the algorithm for cluster head selection and cluster formation is as follows:

Step 1: Initialize the nodes and labels in the system Ri

(i=1, 2, 3...n).

Step 2: Set the potential score (vitality and portability) to every node and label hubs.

Step 3: Send the vitality level of the Reader to Base Station and discover optimum nodes.

Step 4: If (Residual Energy (Ri)> Threshold esteem).

Then: Update the node as an Eligible Cluster Head.

else: Update the nodes as Remaining nodes in the system.

Step 5: Separation is determined for a qualified head in the system utilizing (Eq. (1)).

Step 6: Alignment is determined for the head in the order using Eq. (2).

Step 7: Cohesion is defined as a qualified leader in the system utilizing Eq. (3).

Step 8: Add the estimations of partition, arrangement, and union.

Step 9: If the worth is high, select as "Ideal head."

Step 10: else "Become customary nodes" in the system.

Step 11: End the Cluster development.

In the RFID network, taking into consideration the potential value of the readers, we can determine the optimal cluster head by employing a cluster formation algorithm. To obtain an adequate cluster configuration in the network, some procedures like separation or cohesion are applied.

The optimal set of cluster heads that belong with their associated cluster members are predicted by the base station. In the RFID network, the cluster head plays an important role to send the data from one cluster ID and vice versa. Cluster head also plays a role of local control center to organize this event and cluster base station acted as a Reader arranger.

Regarding data transmission, every reader begins to pass a signal for sensing the information after the cluster formation and cluster head selection. Within the clustering schedule, cluster head works as readers to detect data. The TDMA schedule is utilized in the cluster for arranging the readers. The reader throws the signal to tags with their corresponding range pedestal of the program. The reader sends the information to the cluster head once it senses the information. Subsequently, the next reader begins to pass the data. With the help of a cluster head, each reader finishes the data transmission and data aggregation.

V. Experiment

An object-driven network simulator, network simulator version 2 (NS-2), was developed at the University of California-Berkeley. Such a simulator utilizes two programming languages: C++ and Tcl. NS-2 is useful for the simulation of the wide-area and local networks. These programming languages are used for numerous reasons, most importantly, because of their internal characteristics. While C++ provides efficiency in its implementation of a specific design, it encounters some difficulties in graphic representation. Without a visual language that is easy-to-use and descriptive, it may be challenging to perform a modification and assembly of different components and alter distinct parameters.

The system test system is typically called an NS2; it is a capable test system for concentrating dynamic behavior of portable remote sensor organizers. NS2 boosts the re-enactment of an order from a physical radio transmission channel to the application layer. The NS2.35 test system is utilized for re-enactment and is directed under the Linux mint environment. This testing was conveyed using the standard network test system, NS-2.34, which has 100 nodes. These nodes are spread by an arbitrary request in a 100 x 100 area.

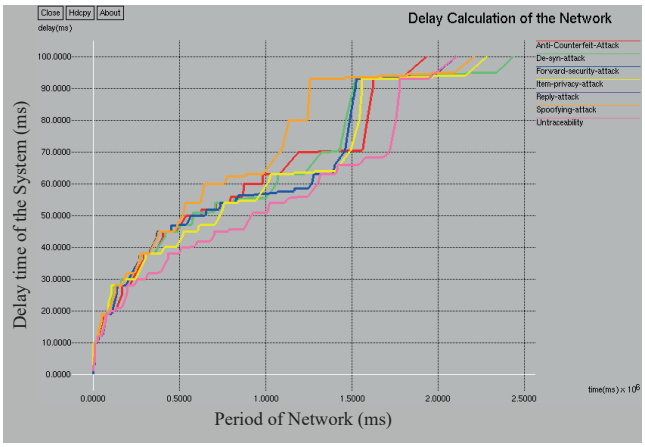

Fig. 5. Delay Calculation of the network.

While using any kind of implementation in the network the throughput must be identified and the latency of the connectivity

should be very less with respect to the implementation done in the present existing methodology. Fig. 5 explains the implementation of the delay calculation in the network. This delay can be identified while connecting the RFID tags to the base station to transform information from one location to another location. The existing system deals with the highest delay problem in connecting the server and with the problem with reconnection when there is any network drop.

In the existing system, several attacks are analyzed, and the results are calculated. Fig. 6 shows the calculation of the throughput of the network. The network throughput is defined as the number of packets transmitted according to the period. Hence, it is a two-dimensional figure that consists of two axes.

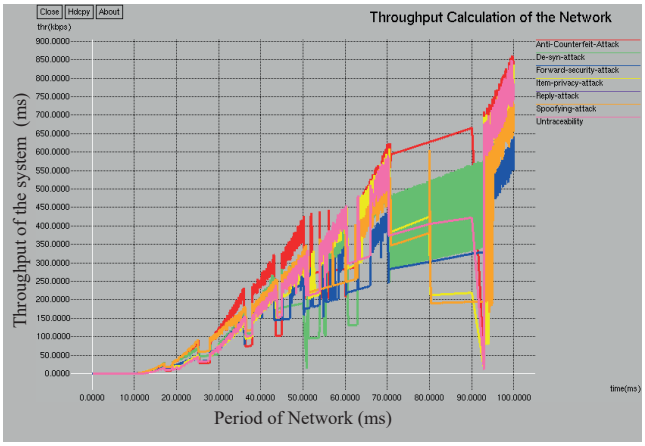

Fig. 6. Throughput Calculation of the network.

The through put can be exhibited with the network connecting time and the data acquisition from different repositories. In this data acquisition we gather data from different knowledge bases and connect the client to the base station.

In the existing system, several attacks are analyzed, and the results are calculated. Fig. 7 shows the calculation of the forwarding security of the network. The forward network security is defined as that the amount of count of security packets in the forward direction according to the time. Hence it is the two-dimensional figure. It consists of two axes.

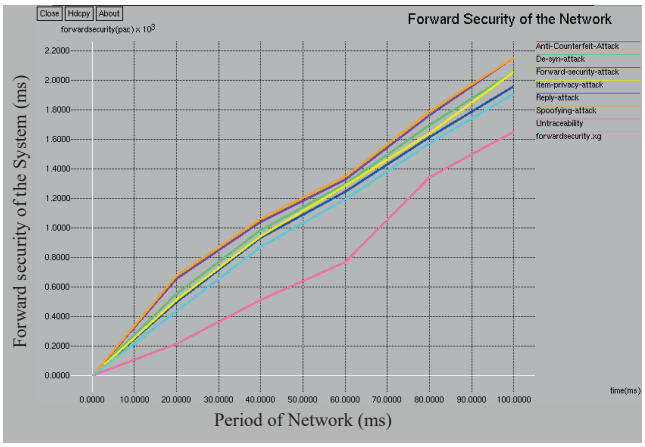

Fig. 7. Forward Security Calculation of the network.

There are different approaches to calculate the threat in the network and the best way to analyses the network security is by maintaining forward network security.

In the existing system, several attacks are analyzed, and the results are calculated. Fig. 8 shows the calculation of the received packets in the network. The network received packages is defined as that the number of packets received by the destination during the transmission of packets from the source to the destination, according to the period. Hence, it is a two-dimensional figure that consists of two axes.

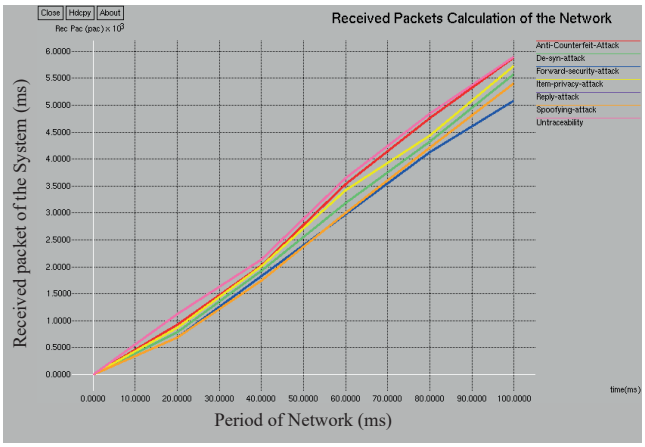

Fig. 8. Received Packets Calculation of the network.

Before completing the transmission we need to calculate the number of packets we are transmitting from one node to another and after completing the transmission we need to check the whether all the packets is received or not.

In the existing system, several attacks are analyzed, and the results are calculated. Fig. 9 shows the calculation of the sent packets in the network. The network sent packages is defined as the number of packets transmitted by the source (sender node) during the transmission of packets from the source and to the destination, according to the period. Hence, it is a two-dimensional figure that consists of two axes.

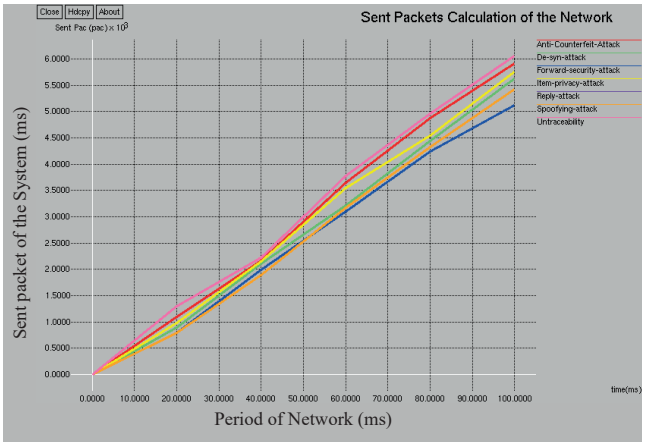

Fig. 9. Sent Packets Calculation of the network.

Fig. 10 shows the calculation of energy consumption, and it is a comparative analysis between the existing and the proposed method. The network energy consumption is defined as the amount of energy utilized or spent during the data transmission between the source and the destination, according to the period, until the end of the communication. Hence, it is a two-dimensional figure that consists of two axes.

Fig. 11 shows the calculation of energy efficiency, and it is a comparative analysis between the existing and the proposed method. The network energy efficiency is defined as the amount of energy saved during the data transmission, between the source and the destination, according to the time period and until the end of the transfer. Hence, it is a two-dimensional figure that consists of two axes.

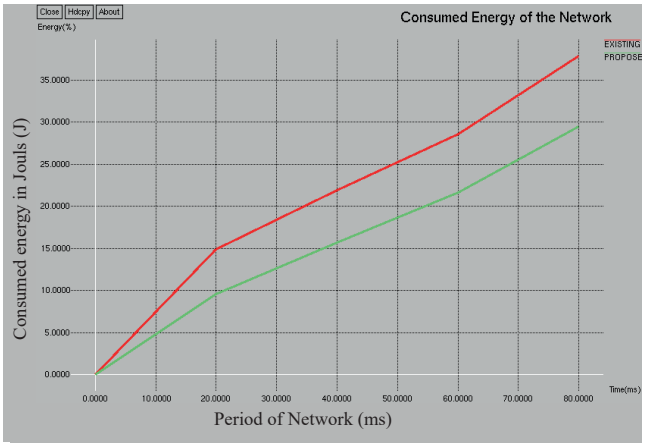

Fig. 10. Consumed Energy Calculation of the network.

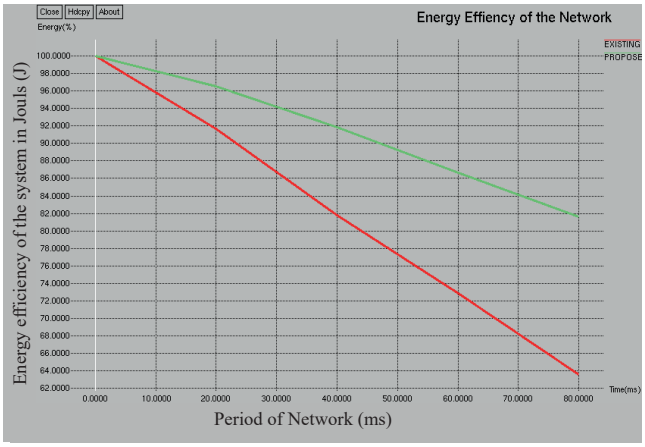

Fig. 11. Energy Efficiency Calculation of the network.

The energy of the network must be identified before performing any kind of operation. In this energy efficiency the network must use the minimum energy and execute the large task.

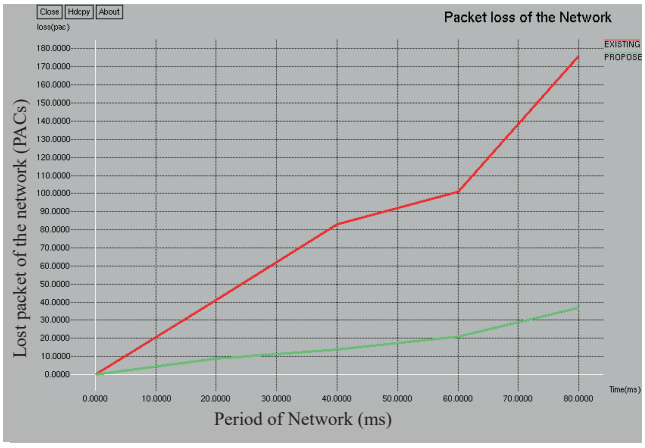

Fig. 12. Packet Loss Calculation of the network.

Fig. 12 shows the calculation of packet loss and is a comparative analysis between the existing and the proposed method. The network packet loss is defined as the number of packets lost during the data transmission between the source and the destination according to the time until the end of the communication. Hence, it is a two-dimensional figure and consists of two axes.

While transmitting the information the task we need to consider is the avoiding packet loss. While transmitting information sometimes because of problem in network establishment packets may loss. We need to avoid and calculate those and recover those.

Fig. 13 shows the calculation of generated packets and is a comparative analysis between the existing and the proposed methods. The system made packets are defined as that the number of packages sent during the data transmission between the source and the destination, according to the time period until the end of the transfer. Hence, it is a two-dimensional figure and consists of two axes.

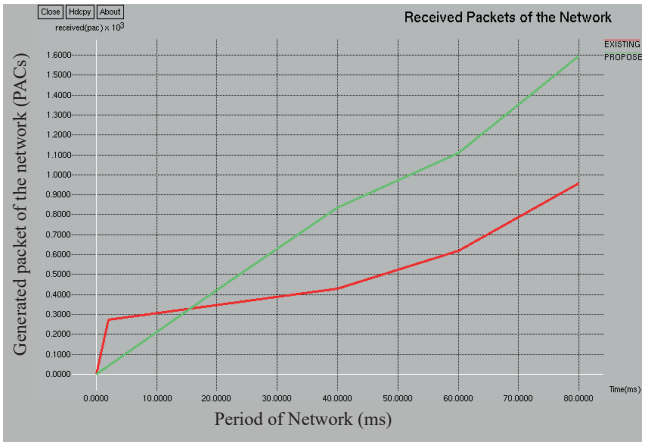

Fig. 13. Generated packets Calculation of the network.

The existing and proposed systems are compared with the service of different network admins while transmitting the information. We need to calculate the packets which are being generated.

Fig. 14 shows the calculation of received packets. This is a comparative analysis between the existing and the proposed methods. The system received packages, defined as the number of packets received during the data transmission between the source and the destination according to the time period and until the end of the transfer. Hence, it is a two-dimensional figure that consists of two axes.

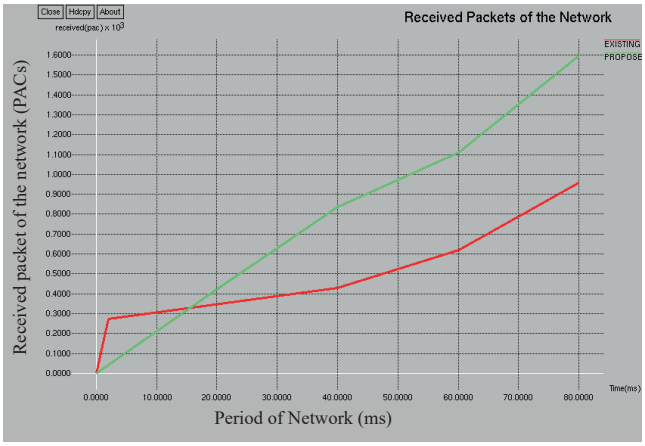

Fig. 14. Received packets Calculation of the network.

Fig.15 shows the calculation of the packet's delivery ratio, and it is a comparative analysis between the existing and the proposed method. The network packets delivery ratio is defined as that the percentage of packets received vs. the number of packages sent during the data transmission between the source and the destination according to the time period till the end of the transfer. Hence it is the two-dimensional figure. It consists of two axes.

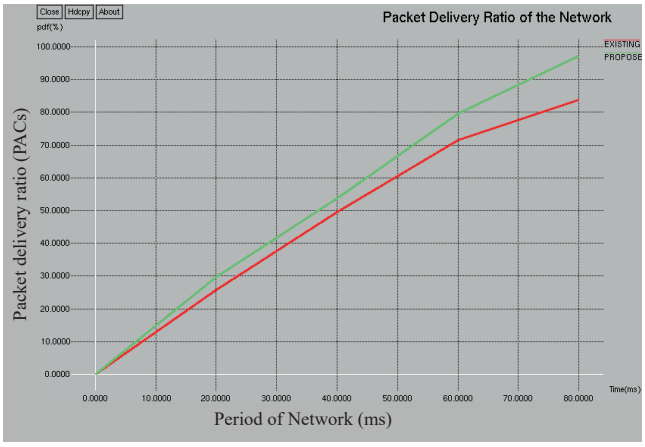

Fig. 15. Packets Delivery Ratio Calculation of the network.

Fig. 16 shows the calculation of throughput, and it is a comparative analysis between the existing and the proposed methods. The network throughput is defined as that the overall calculation of the number of packets sent during the data transmission between the source and the destination, according to the time period and until the end of the transfer. Hence, it is a two-dimensional figure that consists of two axes.

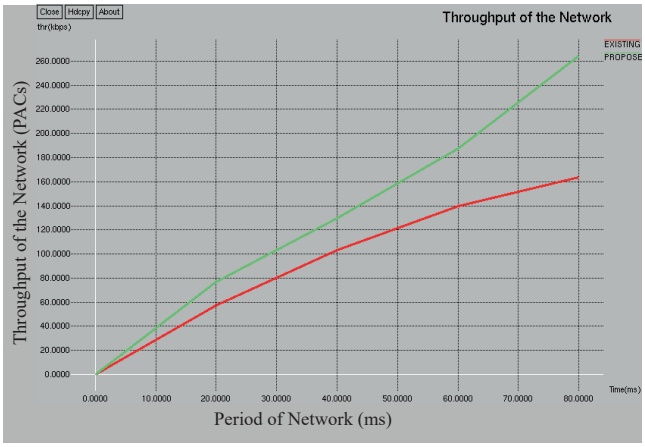

Fig. 16. Throughput Calculation of the network.

VI. Conclusions and Future Work

The network environment is designed and implemented using Network Simulator. The simulator executes the proposed dragonfly clustering protocol for cluster head selection and cluster formation to reduce the cluster breakage and to improve the reading efficiency in the network. In the considered 100 nodes in the network, there are three types of sensors such Readers, tags and cluster heads. All the readers are homogeneous in the cluster but perform different tasks. This type of distribution balances the operational load within each cluster and also results in improved network lifetime. The cluster head schedules data collection time in the network. Readers sense the data from tags and send to cluster head within the cluster. Cluster head performs aggregation of the gathered data before transmitting them to the base station. Our simulation result is evaluated in terms of number of parameters such as network lifetime (number of Active nodes) and cluster head selection rounds.

Earlier work in this domain had tried to provide a genuine solution through malicious attack. Our proposed work is an effort in the same direction. In this work the hash function and public-key encryption with timestamping on either side of a two-way communication are used to remove minimal chances of an attack on a wireless connection.

In the context of future work, it is necessary to emphasize the *IEEE* issue of time complexity; the next step will be to evaluate the time function, and to minimize it to make the system more efficient in a real-time scenario.

References

[1] R. Koh, E. W. Schuster, I. Chackrabarti, and A. Bellman, "Securing the Pharmaceutical Supply Chain," *White Paper MIT-AUTO ID-WH- 021, Auto-Id Center MIT,* Cambridge, MA 02139-4307, USA, 2003, Available at http://www.mitdatacenter.org

[2] J. Kim, D. Choi, I. Kim, and Kim H., "Product authentication service of consumer's mobile RFID device," *IEEE 10th International Symposium on Consumer Electronics*, pp. 1-6, 2006.

[3] Kim, J. and Kim, H., "A wireless service for product authentication in mobile RFID environment", *1st International Symposium on Wireless Pervasive Computing,* pp. 1-5, 2006.

[4] C. –L. Chen, Y. –Y. Chen, T. –F. Shih, T. –M.Kuo, "An RFID Authentication and Anti-counterfeit Transaction Protocol, " *International Symposium on Computer, Consumer and Control*, 2012, pp. 419-422.

[5] S. Pahuja, S. Negi, A. Verma, P. Rathi, N. Narang, R. Chawla, "An Authentication Protocol for secure tag-reader communication," IEEE Students' *Conference on Electrical, Electronics and Computer Science,* 2012.

[6] W. Alsalih, K. Ali, and H. Hassanein, "Optimal distance-based clustering for tag anti-collision in RFID systems," 2008 *33rd IEEE Conference on Local Computer Networks (LCN), Montreal, Que, 2008*, pp. 266-273, doi: 10.1109/LCN.2008.4664179.

[7] Birari S.M., Iyer S., "PULSE: A MAC Protocol for RFID Networks" in Enokido T., Yan L., Xiao B., Kim D., Dai Y., Yang L.T. (eds) *Embedded and Ubiquitous Computing – EUC 2005 Workshops. EUC 2005.* Lecture Notes in Computer Science, vol 3823. Springer, Berlin, Heidelberg.

[8] P.D'Arco and A. De Santis, "On ultralightweight RFID Authentication Protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 4, July/August 2011.

[9] J. Yang, K. Ren and K. Kim, "Security and Privacy on Authentication Protocol for Low-Cost Radio", *Proc. 2005 Symp. Cryptography and Information Security,* 2005.

[10] J. Wang, D.Wang, Y.Zhao, and T. Korhonen, "A Novel Anti-Collision Protocol with Collision based Dynamic Clustering in Multiple-Reader RFID Systems," *International Conference on Applied Informatics and Communications*, 2008, pp. 417-422.

[11] M.V. Bueno Delgado, J. Vales Alonso, F.J. Gonzalez Castaño, "Analysis of DFSA Anti-collision Protocols in passive RFID environment" *2009 35th Annual Conference of IEEE Industrial Electronics,* Porto, 2009, pp. 2610-2617, doi: 10.1109/IECON.2009.5415261.

[12] M.Shuang, Y. Xiao-long, "An Efficient Authentication Protocol for Low-Cost RFID System in the Presence of Malicious Readers" 2012 9th *International Conference on Fuzzy Systems and Knowledge Discovery(FSKD 2012)*, pp. 2111-2114.

[13] S. Pahuja, S. Negi, A. Verma, P. Rathi, N. Narang, R. Chawla, "An Authentication Protocol for secure tag-reader communication," *2012 IEEE Students' Conference on Electrical, Electronics and Computer Science*, Bhopal, 2012, pp. 1-4, doi: 10.1109/SCEECS.2012.6184757.

[14] C. –L. Chen, Y. –Y. Chen, T. –F. Shih, T. –M.Kuo, "An RFID Authentication and Anti-counterfeit Transaction Protocol" *2012 International Symposium on Computer, Consumer and Control*, 2012, pp. 419-422.

[15] M.Shuang, Y. Xiao-long, "An Efficient Authentication Protocol for Low-Cost RFID System in the Presence of Malicious Readers" 2012 9 *International Conference on Fuzzy System and Knowledge Discovery (FSKD 2012)*, pp. 2111-2114.

[16] L. F.Bittencourt, E. R. Madeira, F.Cierre, and L.Buzato, "A path clustering heuristic for scheduling task graphs onto a grid," in 3rd *International Workshop on Middleware for Grid Computing (MGC05)*, 2005.

[17] P. S. Mann, and S. Singh, "Energy-efficient hierarchical routing for wireless sensor networks: a swarm intelligence approach." *Wireless Personal Communications*, vol. 92, no. 2, 2017, pp. 785-805.

[18] M. Mirzaie, and S. M. Mazinani, "MCFL: An energy-efficient multi-

clustering algorithm using fuzzy logic in the wireless sensor networks." *Wireless Networks*, vol. 24, no. 6, pp. 2251-2266, 2018.

[19] M. Elshrkawey, S. M. Elsherif, and M. E. Wahed, "An enhancement approach for reducing energy consumption in wireless sensor networks." *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 2, pp. 259-267, 2018.

[20] P. Lalwani, H. Banka, and C. Kumar, "BERA: a biogeography-based energy-saving routing architecture for wireless sensor networks," *Soft Computing*, vol. *22*, no. 5, pp. 1651-1667, 2018.

[21] S.-C. Wang, "Artificial Neural Network," in *Interdisciplinary Computing in Java Programming, Boston, MA: Springer* US, 2003, pp. 81–100.

[22] V. Estivill-Castro, "Why so many clustering algorithms," *ACM SIGKDD Explore. News*., vol. 4, no. 1, pp. 65–75, Jun. 2002.

[23] B. S. Harish, B. S. Kumar, "Anomaly-based Intrusion Detection using Modified Fuzzy Clustering," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 4, no. 6, pp. 54-59, 2017.

[24] García CG, Núñez-Valdez ER, García-Díaz V, Pelayo G-Bustelo C, Cueva-Lovelle JM. "A Review of Artificial Intelligence in the Internet of Things." *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 5, no. 4, pp. 9-20, 2019.

[25] Bahuguna, Y., D. Punetha, and P. Verma. "An analytic Study of the Key Factors Influencing the Design and Routing Techniques of a Wireless Sensor Network." *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 4, no. 3, pp. 11-15, 2017.

Pramod Singh Rathore

Pramod Singh Rathore is pursuing his Doctorate in computer science & Engineering from Bundelkhand University and research is going on Networking and done M. Tech in Computer Sci. & Engineering from Government engineering college Ajmer, Rajasthan Technical University, Kota India. He has been working as an Assistant professor of Computer Science & Engineering Department at Aryabhatt Engineering College and Research centre, Ajmer, Rajasthan and also visiting faculty in Government University MDS Ajmer. He has total Academic teaching experience of more than 8 years with more than 45 publications in reputed, peer reviewed National and International Journals, books & Conferences like Wiley, IGI GLOBAL, Taylor & Francis Springer, Elsevier Science Direct, Annals of Computer Science, Poland, and IEEE. He has co-authored & edited many books with many reputed publisher like Wiley, CRC Press, USA. .His research area includes NS2, Computer Network, Mining, and DBMS.

Abhishek Kumar

Abhishek Kumar is Doctorate in computer science from University of Madras done M.Tech in Computer Sci. & Engineering from Government engineering college Ajmer, Rajasthan Technical University, Kota India. He has total Academic teaching experience of more than 8 years with more than 60 publications in reputed, peer reviewed National and International Journals. His research area includes- Artificial intelligence, Image processing, Computer Vision, Data Mining, Machine Learning. He has authored 6 books published internationally and edited 16 book with Wiley, IGI GLOBAL Springer, Apple Academic Press and CRC etc. He is also member of various National and International professional societies in the field of engineering & research like Senior Member of IEEE. He has got Sir CV Raman life time achievement national award for 2018 in young researcher and faculty Category.

Vicente García-Díaz

Vicente García-Díaz is an Associate Professor in the Department of Computer Science at the University of Oviedo. He has a PhD in Computer Science from the University of Oviedo and a Diploma in Advanced Studies, as well as Degrees in Computer Engineering and Technical Systems Computer Engineering. In addition, he possesses a Degree in Occupational Risk Prevention. He is part of the editorial and advisory board of several international journals. He has supervised 90+ academic projects and published 90+ research papers in journals, conferences, and books. His teaching areas are algorithm design techniques, and design and development of Domain-Specific languages. His research interests also include decision support systems and the use of technologies in teaching and learning.